Amendments to the Specification:

Please replace the paragraph on page 1, beginning on line 14, with the following paragraph.

With the increased reliance on WLANs, businesses are increasing more concerned about network security. With a WLAN, transmitted data is broadcast over the air using radio waves. This means that any wireless client within an access point (AP) service area can receive data transmitted to or from the access point. Because radio waves travel through ceilings, floors, and walls, transmitted data may reach unintended recipients on different floors or even outside the building that houses the AP. With a WLAN, the boundary for the network has moved. Without stringent security measures in place, installing a WLAN can be the equivalent of putting Ethernet ports everywhere, including the parking lot.

Please replace the paragraph on page 2, beginning on line 17, with the following paragraph.

Figure 1 illustrates the transactions involved in client authentication in the 802.11 specification. Initially, during the "discovery" phase, a mobile node (MN) client 10 broadcasts a probe request frame 20 on several channels. Access points 12 of the wired network 14 within range respond with a probe response frame 22. The client 10 then decides which access point 12 is best for access and sends an authentication request 24 initiating the "authentication" phase. The access point 12 sends an authentication reply 26. Upon successful authentication, the client 10 commences the "association" phase by sending an association request frame 28 to the access point 12. The access point then replies with an association response 30 and, thereafter, the client is then able to pass traffic to and [[and]]receive traffic from the access point.

Please replace the paragraph on page 5, beginning on line 23, with the following paragraph.

Further, the re-associating includes issuing a re-association request by said mobile node MN to the access point AP including signature information indicative of the mobile node MN holding a fresh/live pairwise transient key PTK. The signature information is validated by the

access point AP and a group transient key GTK is delivered from the access point to the mobile node MN ~~to the access point AP~~. The group transient key is used to protect communication between the mobile node MN, the access point AP, and the wireless network WLAN.